REMARKS

Claims 1-29 are under examination. Claims 1, 14, and 24-29 have been amended. No new matter has been added as a result of these claim amendments.

EXAMINER INTERVIEW SUMMARY

On December 29, 2005, Ronald Pomerenke, representative for the Applicants, conducted a telephonic interview with examiner Eleni Shiferaw. Applicants thank the examiner for granting the interview. Claim 1 was discussed with respect to Dougall, Pub.No. 2003/0093485 A1 and Quick, Jr. (Quick, Patent No.: US 6,260,147 B1). No definitive agreements were reached.

REJECTIONS BASED ON CITED ART

Claims 1-7, 11-15, 17-19, and 22-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dougall et al. (Dougall, Pub.No. 2003/0093485 A1) in view of Quick, Jr. (Quick, Patent No.: US 6,260,147 B1). The rejection is respectfully traversed for the following reasons.

Currently Amended Claim 1 recites, in part:

selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol.

Support for the amendment to Claim 1 may be found in the specification at least in paragraphs 46, 47, 49, 50, 66, 82, 95, and 96.

Selecting a subset of data for encryption from a set of data to be communicated between the client and the server in a particular payload allows the selected subset of data to be encrypted and non-selected portions of the data to be communicated between the client and the server in the particular payload to be sent in the clear. For example, a user password to be transferred in a particular payload can be selected for encryption, whereas other information to be transferred in the particular payload (e.g., userID, etc.) is not selected for encryption.

Dougall fails to teach or suggest selecting a subset for encryption from a set of data to be communicated ... in a particular payload. Dougall either encrypts all of the payload (FIG. 20, 920) or none of the payload 920. Dougall fails to teach or suggest that, from a set of data to be communicated ... in a particular payload, a subset of data is selected for encryption, as claimed.

Furthermore, Applicants assert that Quick does not teach or suggest these limitations, while noting that the rejection does not assert that Quick teaches or suggests these limitations. Therefore, the combination of Dougall and Quick fails to teach or suggest these claim limitations.

For the foregoing reasons, the combination of Dougall and Quick fails to teach or suggest the recited limitations, "selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol," as claimed.

II

Currently Amended Claim 1 further recites, in part:

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads, wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads.

Applicants assert that Dougall does not teach or suggest these claim limitations. Moreover, contrary to the rejection's assertion, Quick fails to teach or suggest these limitations. Therefore, the combination of Dougall and Quick fails to teach or suggest these claim limitations.

Quick may teach generating a key that may be unique relative to other generated keys. However, that key is used over and over again throughout the communication session. Therefore, the key is not unique relative to keys associated with other payloads in the communication session.

Quick teaches (col. 3, lines 1-6) that a subscriber enters a user identifier and a password into a terminal when the subscriber wishes to register a terminal to his subscription. Responsive to the subscriber input, the terminal generates a public/private key pair and stores it. Quick teaches that the user identifier and password are used to register a terminal to the user's subscription. Quick does not teach or suggest that the public/private key pair used in connection with transferring a particular payload is unique relative to public/private key pair used in connection with transferring other payloads. Rather, Applicants assume that because

the password is used to register a terminal to a subscription, the same public/private key pair would be used in connection with transferring different payloads associated with the terminal.

The rejection also appears to assert that Quick discloses a session key that teaches the claimed secret integer. A session key is used for an entire session, which may comprise multiple payloads. Therefore, the same session key may be used for different payloads. Thus, the Quick's session key is not, "a secret integer associated with the particular payload [that] is unique relative to secret integers associated with other payloads of the plurality of payloads," as claimed.

For the foregoing reasons, the combination of Dougall and Quick fails to teach or suggest the above recited limitations.

Independent Claims 24, 26 and 28 recite similar limitations to those discussed in the response to Claim 1. For at least the reasons discussed in the response to Claim 1, Claims 24, 26 and 28 are patentable.

Claims 2-7, and 11-13 depend from Independent Claim 1, incorporating limitations therefrom. As explained above, Claim 1 includes limitations that define patentable subject matter. Therefore, these dependant claims recite patentable subject matter for at least the same reasons Claim 1 recites patentable subject matter.

Independent Claim 14 recites, in part:

wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads;

determining the secret integer based, at least in part, on the clue information; and

based on the secret integer, decrypting the encrypted data to generate a subset of data communicated between client and server, wherein the subset is encrypted when transferred from the sending device to the receiving device.

As discussed in part II herein, Quick fails to teach or suggest, "wherein the secret integer associated with the particular payload is unique relative to secret integers associated with other payloads of the plurality of payloads," as claimed. Moreover, for at least the reasons discussed in part II in the response to Claim 1, the combination of Dougall and Quick fails to teach or suggest these claim limitations.

Independent Claims 25, 27 and 29 recite similar limitations to those discussed in the response to Claim 14. For at least the reasons discussed in the response to Claim 14, Claims 25, 27 and 29 are patentable.

Claims 15, 17-19 and 22-23 depend from Independent Claim 14, incorporating limitations therefrom. As explained above, Claim 14 includes limitations that define patentable subject matter. Therefore, these dependant claims recite patentable subject matter for at least the same reasons Claim 14 recites patentable subject matter.

Claims 8-10, 16, and 20-21 were rejected under 35 U.S.C. 103(a) as being unpatentable over Dougall, in view of Quick, in further view of Carman et al. U.S. Published Patent Application No. 2002/0199102 ("Carman").

Claims 8-10, 16 and 20-21 depend from Independent Claim 1 or Independent Claim 14, incorporating limitations therefrom. As explained above, these independent claims include limitations that define patentable subject matter over Dougall and Quick. Carmen is used as allegedly teaching applying a hash function and as allegedly teaching determining a shared secret key based on clue information. However, Carmen is not alleged to nor does Carmen remedy the deficiencies of Dougall and Quick discussed herein. Therefore, Independent Claims 1 and 14, along with claims dependent therefrom, are allowable over the combination of Dougall, Quick, and Carmen.

CONCLUSION

The Applicants believe that all issues raised in the Final Office Action have been addressed and that allowance of the pending claims is appropriate.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicants petition for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Date: December 30, 2005

Ronald M. Pomerenke
Reg. No. 43,009

2055 Gateway Place, #550
San Jose, CA 95110
Telephone: (408) 414-1080, ext. 210
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on December 30, 2005 by

Judy Paradoski